

**AFFIDAVIT IN SUPPORT OF APPLICATIONS  
FOR SEARCH AND SEIZURE WARRANTS**

I, Raymond J. StClair, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer (“TFO”) of the Drug Enforcement Administration (“DEA”) assigned to the DEA Dayton Resident Office since January 2019. I, therefore, am an “Investigative or Law Enforcement Officer” of the United States within the meaning of Title 21, United States Code, Section 878, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 21, United States Code, Section 878.

3. I am a law enforcement officer and have been employed by the Dayton Police Department since 2000 and have been assigned to the Narcotics Bureau since January 2005. I have been assigned as a TFO with the DEA since January 2019. I have extensive prior experience in investigating drug cases that resulted in successful prosecution of persons involved in trafficking of drugs, possession of drugs, and other related offenses. I have been involved in narcotics related arrests, executed search warrants that resulted in the seizure of narcotics, participated in undercover narcotics purchases and supervised the activities of informants who have provided information and assistance resulting in narcotics purchases. Through training and experience, I

am familiar with the manner in which persons involved in the illicit distribution and sales of controlled substances often operate. These subjects usually attempt to conceal their identities, as well as the locations at which they reside and where they store controlled substances and the illegal proceeds derived therefrom. Through training and experience, I am familiar with the practices of narcotics distributors and sellers, whereby they attempt to conceal the true nature, source and location of proceeds of illegal activity, commonly referred to as money laundering. It has been my experience while conducting other drug investigations that individuals operating drug houses and/or apartments continue to diversify and it is not uncommon to recover different types of illegal drugs from inside the residence. It is also not uncommon to encounter individuals in possession of illegal drugs after leaving from operating drug houses/apartments. In addition, it has been my experience that firearms are commonly kept and located inside operating drug houses and/or apartments.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched are as follows:
  - a. Kyocera Model: E4610, IMEI: 990006153340772 (hereinafter referred to as “**Subject Device-1**” and more fully described in Attachment A).
  - b. iPhone (black), Model: unknown, Serial Number: unknown (hereinafter referred to as “**Subject Device-2**” and more fully described in Attachment A).
  - c. iPhone 6S, Model: A1633, IC: 579C-E2946A (hereinafter referred to as “**Subject Device-3**” and more fully described in Attachment A).
  - d. iPhone 7, Model: A1660, IC: 579C-E3085A (hereinafter referred to as “**Subject Device-4**” and more fully described in Attachment A).

e. iPhone 7 Plus, Model: A1661, IC: 579C-E3087A (hereinafter referred to as “**Subject Device-5**” and more fully described in Attachment A).

f. Kyocera Model: E4610, IMEI: 990006159262111, with additional SIM card attached to exterior of phone (serial number: 89148 00000 56742 24514) (hereinafter referred to as “**Subject Device-6**” and more fully described in Attachment A).

g. iPhone 6, Model: A1586, IMEI: 353027099559805 (hereinafter referred to as “**Subject Device-7**” and more fully described in Attachment A).

h. ATT Radiant Core, Model: U304AA, IMEI: 863382042874881 (hereinafter referred to as “**Subject Device-8**” and more fully described in Attachment A).

i. Samsung with blue case, Model: Unknown, IMEI 351767112592414 (hereinafter referred to as “**Subject Device-9**” and more fully described in Attachment A).

5. **Subject Device-1** through **Subject Device-9** are currently located in the custody of the DEA at their offices located at 3821 Colonel Glenn Highway, Beavercreek, Ohio.

6. The applied-for warrant would authorize the forensic examination of **Subject Device-1** through **Subject Device-9** for the purpose of identifying electronically stored data particularly described in Attachment B.

#### **PROBABLE CAUSE**

7. Since February 2019, the DEA Dayton Resident Office and the Dayton Police Department are conducting a joint investigation into a drug trafficking organization, which is distributing fentanyl, methamphetamine, among other drugs, in the Southern District of Ohio. During the course of subject investigation, agents identified Paul DORSEY, Antone DORSEY, Angelo TURPIN, and others as members of this drug trafficking organization.

8. Based on surveillance performed on members of the drug trafficking organization (DTO) and through utilization of other investigative techniques, investigators identified 15 Brookhaven Drive, Trotwood, Ohio 45426 as a location utilized by the drug trafficking organization to maintain drugs and other drug trafficking materials. During surveillance, law enforcement has observed other known members of the DTO, not referenced here, at 15 Brookhaven Drive by investigators.

9. On May 5, 2021, law enforcement executed a federal search warrant signed by the Honorable Judge Sharon L. Ovington at 15 Brookhaven Drive, Trotwood, Ohio 45426. Paul DORSEY, Antone DORSEY, and Angelo TURPIN were located at this location. Paul DORSEY, Antone DORSEY, and Angelo TURPIN were holding cellular phones when they were located. During the search of this location, investigators located additional cellular phones in or next to the beds and couches where Paul DORSEY, Antone DORSEY, and Angelo TURPIN reportedly slept. Law enforcement also located a firearm, suspected methamphetamine, US currency in denominations consistent with retail drug trafficking, and drug processing equipment such as, but not limited to, digital scales with drug residue and utensils for mixing/cutting narcotics. Law enforcement located **Subject Device-1, Subject Device-2, Subject Device-3, Subject Device-4, Subject Device-5, Subject Device-6, Subject Device-7, Device-8, and Subject Device-9** as described in paragraph 3 above and in Attachment A, in 15 Brookhaven Drive, Trotwood, Ohio 45426.

10. Based on training and experience, I know that drug traffickers frequently use wireless/cellular phones to carry out their activities. They use cellular phones to communicate with customers, their associates, and their suppliers. It is often common for drug traffickers to have multiple phones because certain phones may be used only for certain purposes. For instance,

a trafficker may use one phone just to speak to his supplier, while using a different phone to speak only to his customers. This is a counter-surveillance technique intended to make it harder for law enforcement to identify the user of the phones and his associates. Of the other known members of the DTO who had been observed at 15 Brookhaven Drive, one of the members had previously sold methamphetamine to an undercover officer during this investigation where the member used a cellular phone to complete the drug transaction. Of the phone numbers known to this investigator which are associated to members of the DTO, phone toll analysis showed the members had been in contact with each other and known sources for narcotics locally and from other states. The number of phones located at the address is consistent with the multiple phone use I have observed in other drug investigations.

11. Based on my training and experience, drug traffickers commonly use prepaid cellular phones to hide their identity as the user because they generate no billing information, often require little to no identifying information to activate, can sometimes be activated using an alias, and can be easily disposed of should the trafficker believe that law enforcement has identified the phone number.

12. I also know that traffickers commonly text message each other or their customers, such as meeting locations, prices, and other information needed to carry out the sale of drugs (sometimes in code). They commonly store phone numbers for their associates and customers in the electronic phone book/contacts list, often under alias or code names. I know that traffickers, using digital cameras located on their cellular phone, will sometimes use the cellular phone to take photographs or videos of themselves, their location, their product, their firearms or their associates, which can be electronically stored on the cellular phone. Information can also be downloaded from the internet onto the cellular phone, such as email, social network information (like

“Facebook”), travel information like maps or directions, or photographs. Call data, such as missed calls, received calls, or dialed calls are often electronically stored in the cellular phone. The information electronically stored on a phone can also be evidence of who possessed or used a cellular phone at a given time, can contain direct evidence of drug trafficking acts, and can help identify drug trafficking locations or associates through GPS data. I am aware that there are tools to extract electronic data from a cellular phone so that law enforcement can review it for items of evidentiary value.

13. **Subject Device-1** through **Subject Device-9** are currently in the lawful possession of the DEA. The subject devices came into the DEA’s possession in the following way: taken during the execution of the federal search warrant as described above in Paragraph 9. Therefore, while the DEA might already have all necessary authority to examine **Subject Device-1** through **Subject Device-9**, I seek this additional warrant out of an abundance of caution to be certain that an examination of **Subject Device-1** through **Subject Device-9** will comply with the Fourth Amendment and other applicable laws.

14. **Subject Device-1** through **Subject Device-9** are currently in storage in the custody of the DEA at their offices located at 3821 Colonel Glenn Highway, Beavercreek, Ohio. In my training and experience, I know that **Subject Device-1** through **Subject Device-9** have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when **Subject Device-1** through **Subject Device-9** first came into the possession of the DEA.

#### TECHNICAL TERMS

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.



- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.



- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a

telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

- h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available online at <http://www.apple.com>, I know that **Subject Devices 2, 3, 4, 5, and 7** have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, has internet capabilities, allows the downloading and use of software applications and as a PDA (such as but not limited to: messaging, emails, and storage of documents, passwords, notes, and credit card information). Consulting the manufacturer’s advertisements and product technical

specifications available online at <https://www.kyoceramobile.com>, I know that **Subject Device-1** and **Subject Device-6** have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, has internet capabilities, allows the downloading and use of software applications and as a PDA (such as but not limited to: messaging, emails, and storage of documents, passwords, notes, and credit card information). Consulting the manufacturer's advertisements and product technical specifications available online at <http://www.samsung.com>, I know that **Subject Device-9** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, has internet capabilities, allows the downloading and use of software applications and as a PDA (such as but not limited to: messaging, emails, and storage of documents, passwords, notes, and credit card information). Consulting the manufacturer's advertisements and product technical specifications available online at <http://www.att.com>, I know that **Subject Device-8** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, has internet capabilities, allows the downloading and use of software applications and as a PDA (such as but not limited to: messaging, emails, and storage of documents, passwords, notes, and credit card information).

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence

of the crimes described on the warrant, but also forensic evidence that establishes how each of the devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

//

//

//

//

//

//

//

//

**CONCLUSION**

21. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of **Subject Device-1, Subject Device-2, Subject Device-3, Subject Device-4, Subject Device-5, Subject Device-6, Subject Device-7, Subject Device-8, and Subject Device-9** described in Attachment A to seek the items described in Attachment B.

  
\_\_\_\_\_  
Task Force Officer Raymond J. St.Clair  
Drug Enforcement Administration

Subscribed and sworn to me this 13<sup>th</sup> day of May, 2021.

  
\_\_\_\_\_  
Sharon L. Ovington  
United States Magistrate Judge



**ATTACHMENT A**

**ITEM TO BE SEARCHED**

**Subject Device-1** is a Kyocera, E4610, IMEI: 990006153340772, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The Kyocera wireless telephone is further depicted in the following photograph.





**ATTACHMENT A**

**ITEM TO BE SEARCHED**

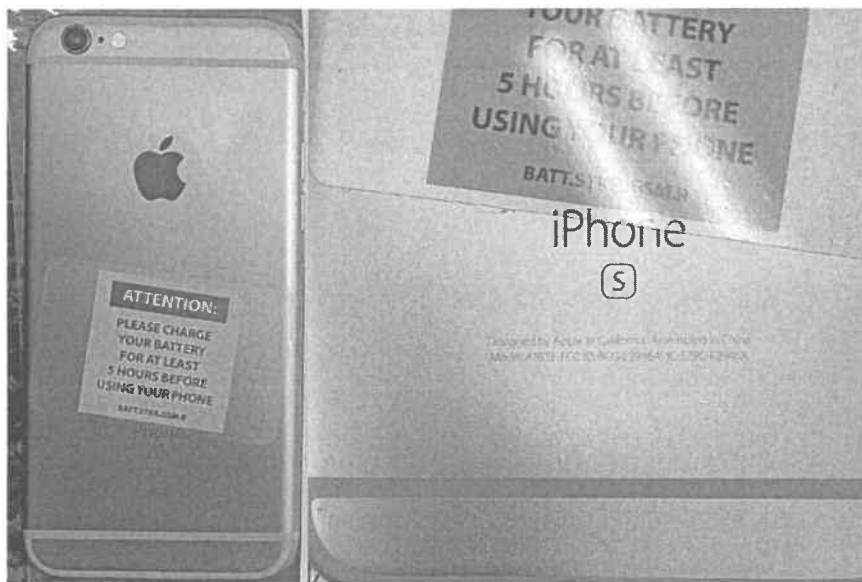
**Subject Device-2** is an iPhone (black), Model: unknown, Serial Number: unknown, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The iPhone wireless telephone is further depicted in the following two photographs.



**ATTACHMENT A**

**ITEM TO BE SEARCHED**

**Subject Device-3** is an iPhone 6S, Model: A1633, IC: 579C-E2946A, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The iPhone wireless telephone is further depicted in the following two photographs.



**ATTACHMENT A**

**ITEM TO BE SEARCHED**

**Subject Device-4** is an iPhone 7, Model: A1660, IC: 579C-E3085A, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The iPhone wireless telephone is further depicted in the following photograph.



**ATTACHMENT A**

**ITEM TO BE SEARCHED**

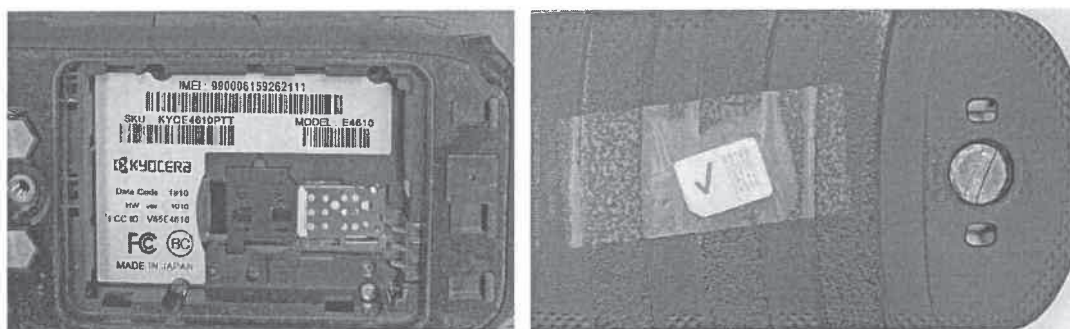
**Subject Device-5** is an iPhone 7 Plus, Model: A1661, IC: 579C-E3087A, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The iPhone wireless telephone is further depicted in the following three photographs.



**ATTACHMENT A**

**ITEM TO BE SEARCHED**

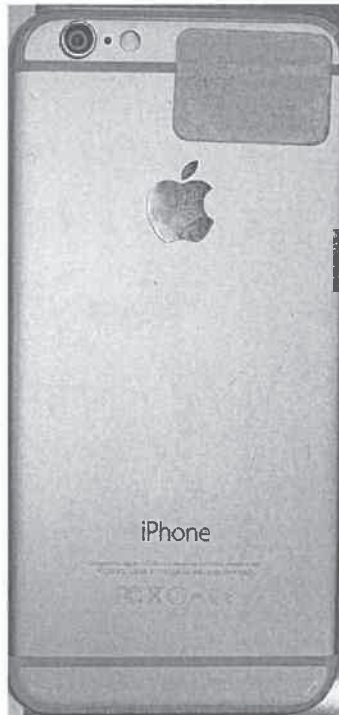
**Subject Device-6** is a Kyocera Model: E4610, IMEI: 990006159262111, with additional an SIM card attached to exterior of phone (serial number: 89148 00000 56742 24514), wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The Kyocera wireless telephone is further depicted in the following two photographs.



**ATTACHMENT A**

**ITEM TO BE SEARCHED**

**Subject Device-7** is an iPhone 6, Model: A1586, IMEI: 353027099559805, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The iPhone wireless telephone is further depicted in the following photograph.



**ATTACHMENT A**

**ITEM TO BE SEARCHED**

**Subject Device-8** is an ATT Radiant Core (black), Model: U304AA, IMEI: 863382042874881, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The ATT wireless telephone is further depicted in the following photograph.





**ATTACHMENT A**

**ITEM TO BE SEARCHED**

**Subject Device-9** is a Samsung with blue case, Model: Unknown, IMEI 351767112592414, wireless telephone, and is currently located at the Drug Enforcement Administration, 3821 Colonel Glenn Highway, Beavercreek, Ohio. The Samsung wireless telephone is further depicted in the following two photographs.



**ATTACHMENT B**

1. All records on **Subject Device-1** through **Subject Device-9** described in Attachment A that relate to violations of 21 U.S.C. §§ 841(a)(1) and 846 (possession with intent to distribute narcotics and conspiracy to commit the same) and involve Paul DORSEY, Antone DORSEY, and Angelo TURPIN since February 2019 including:

- a. lists of customers and related identifying information;
- b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- d. any communications between the user(s) of the Subject Device(s) and customers, suppliers, or other associates related to drug trafficking;
- e. any information recording the schedule or travel of Paul DORSEY, Antone DORSEY, Angelo TURPIN or other user(s) from February 2019 to the present;
- f. any images or video of drugs, large amounts of money, and/or firearms; and
- g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned **Subject Device-1** through **Subject Device-9** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copies pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the DEA may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.